PROBLEM
DRIVEN
RESEARCH

advanced series
Foundation

CONSUMER GOODS & RETAIL 2

AÑO 2013 No. 02

Soluciones de Seguridad
en Gran Consumo y Retail

IE FOUNDATION ADVANCED SERIES ON PROBLEM-DRIVEN RESEARCH

ERNST & YOUNG
Quality In Everything We Do

ie foundation

bienvenida

Estimados Amigos:

Me gustaría presentaros la nueva iniciativa de Fundación IE junto con IE Business School, con la que esperamos proporcionar una nueva forma de presentar los resultados del trabajo conjunto entre nuestros investigadores y las empresas.

IE Business School tiene como uno de sus objetivos ser un centro de excelencia internacional para la investigación en todos los ámbitos de la administración de empresas. Perseguimos este objetivo en estrecha colaboración con Fundación IE y con la recientemente creada IE Universidad.

Con la iniciativa "IE Foundation advaced series on problem driven research" queremos dar un apoyo a las organizaciones que se enfrentan a lo que, más allá de una crisis, parece una nueva estructura económica, con nuevas reglas de mercado. Con este enfoque hemos querido comenzar con la serie "Consumer Goods & Retail" al tratarse del sector que sirve de primer termómetro de la situación y las expectativas sociales.

Mientras que desde IE Business School aportamos al tejido productivo el mejor talento, desde Fundación IE queremos cerrar el círculo virtuoso potenciando una relación sostenible de la escuela con la sociedad a través de las organizaciones.

Confiamos en que esta serie de trabajos cumpla con este reto y ofrezca una perspectiva novedosa sobre las temáticas tratadas.

Marco Trombetta
Vice-Decano de Investigación del IE Business School
Vicerrector de Coordinación e Investigación en IE Universidad

ie foundation

índice

Investigador principal

Álvaro Arenas Sarmiento

Profesor de Sistemas de Información y
Director del Departamento de Sistemas de Información y Tecnologías del IE Business School.

Álvaro Arenas es Profesor de Sistemas de Información y Director del Departamento de Sistemas de Información y Tecnologías del Instituto de Empresa Business School. Tiene un Máster y un Doctorado en Computación de Oxford University, Reino Unido, así como una Licenciatura y un Máster en Ingeniería de Sistemas y Computación de la Universidad de los Andes, Colombia.

Su principal tema de investigación es el manejo de la confianza y la seguridad en sistemas de información distribuidos. Los resultados de su investigación han sido publicados en revistas académicas de alto nivel tales como IEEE Computer, Security and Communication Networks Journal, Internet Computing y Springer Journal of Grid Computing, entre otros.

El profesor Arenas es miembro del Consejo Asesor Científico del proyecto europeo Contrail y lidera el tema de "confianza y seguridad en los sistemas distribuidos a gran escala" dentro del grupo de trabajo ERCIM CoreGRID. Fue coordinador científico del proyecto europeo GridTrust, y responsable del tema de seguridad en el proyecto europeo XtreemOS. Ha sido "keynote speaker" sobre temas de seguridad en Clouds y Grids en conferencias como CloudComp 2010, CCC 2009 y CLEI 2005.

Rafael Puyol
Vicepresidente
Fundación IE

Margarita Velásquez
Directora General
Fundación IE

ie foundation

La Fundación IE tiene entre sus actividades prioritarias el apoyo a la actividad investigadora y a la divulgación del conocimiento de los profesores de la IE Business School. A través de sus iniciativas contribuye a que la Escuela de Negocios se posicione como un centro de excelencia en la innovación y creación de nuevo conocimiento dirigido a su entorno organizativo y productivo.

La Fundación IE pretende crear vínculos estables y alianzas con instituciones de prestigio, tanto públicas como privadas, particularmente del ámbito empresarial, para impulsar la iniciativa de nuestros investigadores. En una institución que persigue la excelencia, las tareas de investigación están presididas por el rigor académico, pero al mismo tiempo por un carácter utilitario que pretende generar conocimiento, impulsar la innovación y competitividad del sector productivo y dar respuesta a los retos y necesidades de la sociedad.

Esta publicación forma parte de la colección sobre Gran Consumo y Distribución que se realiza en la Fundación con el apoyo de Ernst & Young, de quien destacamos su compromiso y su experiencia en este ámbito de conocimiento y a quien queremos expresar nuestro agradecimiento.

La colección se ha diseñado con el propósito de analizar los aspectos claves del sector a través de una visión práctica y actualizada de las tendencias en cuestiones esenciales como Sostenibilidad, Seguridad en la Información, Gestión de Precios y Gestión de la Merma. Estamos en presencia de un ámbito sometido a un intenso proceso de cambio. El reto de la empresa española es estar a la vanguardia de dichos cambios, tomando como referencia las mejores prácticas del mercado global y, desde Fundación IE, queremos acompañar a las empresas en este proceso.

En la confianza de que esta publicación sea de vuestro interés, agradecemos vuestro apoyo.

José Luis Ruíz Expósito
Socio Responsable del Sector
Productos de Consumo y Retail

Manuel Fernández
Director de Desarrollo del Sector
Productos de Consumo y Retail

ERNST & YOUNG
Quality In Everything We Do

Las compañías del sector de gran consumo y distribución están desarrollando su actividad en un entorno económico mucho más complejo y volátil que el de etapas anteriores. En este contexto, las actuaciones más comunes en las compañías del sector se centran en la transformación de los procesos de negocio y la defensa del margen operativo.

En su compromiso con la innovación y la creación de valor, Ernst & Young, junto con la Fundación IE Business School han impulsado aulas de investigación sobre los temas que, consideramos, ayudarán a afrontar los retos planteados al sector.

Entre otras cuestiones, investigamos y proponemos diferentes líneas de actuación en materia de dinámica de precios, desde una perspectiva de oferta diferenciada para las marcas; abordamos el perjuicio económico que supone la llamada "pérdida desconocida" con un enfoque analítico, que nos permite identificar sus orígenes y proponer medidas correctoras para su mitigación ("profit protection"); buscamos respuestas y actuaciones concretas que preserven la seguridad de la información de un sector que opera, cada vez con más frecuencia, en escenarios y tecnologías de movilidad; y proponemos la adopción de una perspectiva de compromiso empresarial, para apostar por una sostenibilidad impulsada por las cadenas de distribución que implique a fabricantes y consumidores.

Estos cuatro ámbitos están experimentando un intenso proceso de cambio. Los estudios de Ernst & Young y la Fundación IE Business School los abordan desde una perspectiva retadora y novedosa, con la intención de que puedan ser llevados a su aplicación práctica y representen un valor añadido para el escenario empresarial.

Resumen ejecutivo

Las tecnologías están cambiando continuamente y, en consecuencia, la forma en que las personas hacen un uso cotidiano de ellas. Cloud Computing, los medios sociales y los dispositivos móviles ya se encuentran integrados en mayor o menor medida en nuestras vidas. ¿A qué nuevos riesgos se enfrentan las compañías al implementar estas nuevas tecnologías para el uso de sus empleados y de sus clientes?

En el presente estudio se analizan estas tecnologías en el contexto del sector de Productos de Consumo y Retail, se muestra a qué nuevos riesgos se exponen las compañías ante estos cambios propiciados por la evolución tecnológica, y qué acciones recomendamos tomar para mitigarlos.

Las empresas del sector requieren adoptar estas nuevas tecnologías para seguir siendo competitivas. Sin embargo, este tipo de cambios en los modelos de negocio que aumentan la exposición al riesgo, siempre deben ser implantados de forma controlada y, en consecuencia, se han de adoptar las medidas necesarias para evitar los nuevos problemas a los que se enfrentan las empresas.

En el caso de Cloud Computing, las principales áreas de riesgo incluyen la integridad y privacidad de los datos, el cumplimiento regulatorio, y la gestión de proveedores de servicios Cloud.

Entre nuestras recomendaciones están la claridad en las políticas de seguridad y la gobernanza del proveedor, elaborar planes de continuidad, y el uso de estándares de seguridad y de la industria.

En las redes sociales encontramos riesgos de seguridad y reputacionales, entre otros. Recomendamos desarrollar una estrategia de protección en los medios sociales que incluya claramente el apoyo de la alta dirección, definir políticas y guías de uso, desarrollar estrategias de monitorización de los medios sociales y un proceso de respuesta a incidentes.

Entre los riesgos en el uso de dispositivos móviles encontramos el robo o pérdida de los dispositivos, la administración de los dispositivos por parte de los usuarios, y la existencia de software malicioso vía aplicaciones. Se recomienda, entre otros, claras políticas que regulen el uso de los dispositivos móviles, implantar seguridad a nivel de dispositivos, y realizar programas de concienciación entre los empleados.

Finalmente, la fuga de datos es un reto común a todas estas tecnologías. Recomendamos a las empresas identificar y clasificar qué datos se consideran sensibles para el negocio, evaluar riegos en todos los canales de comunicación existentes, definir con claridad el flujo de datos que viajan a terceras partes, y establecer un programa de respuesta a incidentes.

1. Tendencias tecnológicas en el sector *Productos de Consumo y Retail*

En una tarde fría de un sábado de noviembre, Amanda, una chica madrileña de 30 años, necesita ropa de verano para sus próximas vacaciones en el Caribe. Hace varios años, Amanda hubiese ido al centro comercial más cercano. Hoy día, inicia la búsqueda de la ropa en Internet, desde la comodidad del sofá de su casa.

Empieza visitando el blog de Rita, una de las blogueras influyentes en el sector moda para conocer cuáles son las últimas tendencias. Luego inicia una sesión de "chat" con el consejero personal virtual de UltimaModa, una de sus tiendas favoritas de la que es cliente. El consejero personal es un agente de software que contrasta los datos de últimas tendencias con el historial de compras de Amanda, historial que se encuentra almacenado en el Cloud de la empresa, para recomendarle artículos de acuerdo a sus preferencias. El consejero le recomienda varios artículos y sobrepone fotografías de éstos sobre el avatar de Amanda. Amanda selecciona dos artículos pero, antes de la compra, cambia a otra pestaña del navegador para buscar comentarios de otros clientes sobre los artículos en las redes sociales y comparar el precio ofrecido con el precio en otras tiendas. Finalmente decide comprar uno de los artículos en UltimaModa y el otro artículo en otra tienda que lo ofrece a un precio menor.

Amanda optó por la opción de recoger el artículo en la tienda de UltimaModa cercana a su trabajo. Al recoger el artículo, encuentra unas sandalias que le gustan. Escanea el código de barras de las sandalias con su smartphone y descubre el mismo por 30 euros más barato en otra tienda. El vendedor le ofrece rápidamente igualar el precio. Amanda no está segura, por lo que le toma la foto a las sandalias y se la envía a tres amigas para que le den su opinión. Las respuestas llegan rápido, todas positivas, por lo que Amanda decide comprar las sandalias.

El escenario descrito anteriormente es ficticio y está inspirado en el escenario presentado en el artículo "The Future of Shopping"[1] de Harvard Business Review*, en su edición especial sobre el sector *Productos de Consumo y Retail* de diciembre de 2011. Sin embargo, todo está basado en opciones reales. Toda la tecnología que Amanda está utilizando está ya disponible, y dentro de unos pocos años gran parte de la tecnología será de uso masivo. El consejero virtual de UltimaModa utiliza datos de los clientes almacenados por la compañía en Cloud para realizar recomendaciones. Los medios sociales han creado un ecosistema donde conversan los clientes sobre los productos que ofrece una marca. Los dispositivos móviles están transformando totalmente el panorama de las empresas, extendiendo los límites de la empresa y ofreciendo a los clientes un acceso ubicuo a información sobre sus productos.

Como vemos en el escenario, las tecnologías de la información y las innovaciones tecnológicas siguen transformando el sector *Productos de Consumo y Retail,* trayendo nuevas oportunidades y retos para los CIOs del sector. CompTIA, la asociación americana de la industria de TI, realizó un estudio el verano pasado entre 500 empresas americanas del sector[2], encontrando que el 72% de las empresas califica la tecnología como importante para el negocio, con una proyección a aumentar dicha proporción a un 83% para el año 2014. Pero el estudio también indica que un

*Las referencias a otras publicaciones se encuentran reunidas al final del documento.

gran número de empresas no ha tenido éxito en el uso de la tecnología. Sólo el 7% de las empresas afirman estar exactamente donde quieren estar en el uso de la tecnología, mientras que el 29% se califica a sí mismo como muy cerca. El estudio de compTIA identifica como principales tendencias tecnológicas para el sector temas como señalización digital, software social, geo-localización y pagos con móviles, entre otros.

En este documento se analizan tres de las tecnologías que están transformando el sector *Productos de Consumo y Retail: Cloud Computing,* medios sociales y tecnologías móviles. La información base para el estudio son investigaciones previas realizadas por Ernst & Young, las cuales se contextualizan para el sector *Productos de Consumo y Retail,* y una investigación realizada conjuntamente entre IE Business School y Ernst & Young entre las principales empresas líderes del sector en España. Analizamos cada tecnología desde el punto de vista de la seguridad de la información, identificando para cada una de ellas las ventajas que ofrece, los retos en su adopción, y presentamos una serie de recomendaciones sobre cómo los CIOs pueden utilizar la tecnología de forma segura y confiable. Un área importante y transversal a las tecnologías es la fuga de datos, la cual se analiza al final del documento, y se recomienda una serie de pasos para mitigar sus potenciales riesgos para el negocio.

2. *Cloud Computing* en el sector *Productos de Consumo y Retail*

Impulsadas por las presiones para reducir el gasto en TI en la estela de la crisis económica, muchas empresas están buscando fuera de la organización ayuda para ser más eficientes. El principal interés se ha centrado en servicios informáticos que requieran una inversión inicial mucho menor, menos recursos internos de TI y menores costes de funcionamiento. Como resultado de ello, los servicios basados en *Cloud Computing* están ganando una mayor adopción.

Cloud Computing es un nuevo paradigma en el que recursos informáticos o de almacenamiento que antes se encontraban en ordenadores de las empresas son ahora alquilados y gestionados por terceros[3]. El modelo de negocio de los proveedores de servicios *Cloud* incluye compartir la infraestructura tecnológica entre varios usuarios así como gestionar el desempeño de los sistemas usando técnicas basadas en virtualización y migración de datos a lo largo de un gran número de equipos que pueden estar ubicados en diferentes sitios geográficos. Los usuarios del Cloud no saben donde están localizados sus aplicaciones o datos, sólo que están en algún lugar en la nube.

Compartir la infraestructura tecnológica conlleva economías de escala tanto a nivel de *hardware como de software*. Los servicios de *software* pueden obtener una escalabilidad casi infinita y un crecimiento incremental de acuerdo a las necesidades de los clientes. Los servicios se pagan siguiendo usualmente el modelo estándar de *"pay-as-you-go"*.

El principal cambio en la transición de una infraestructura de TI desarrollada en casa al *Cloud* es el cambio en la gestión de la calidad y disponibilidad del servicio a través de contratos y relaciones con terceros. Las organizaciones se enfrentan a la necesidad de entender mejor las dependencias entre los diferentes sistemas propios, los cuales muy probablemente han sido desarrollados en años o aun décadas, con el fin de gestionar procesos que combinen servicios de la propia infraestructura con servicios en la nube. Las organizaciones también deben considerar cómo la transición a un *Cloud Computing* externo afecta el riesgo del negocio, especialmente en lo que respecta a la seguridad de datos, privacidad, disponibilidad, así como el cumplimiento regulatorio y legal.

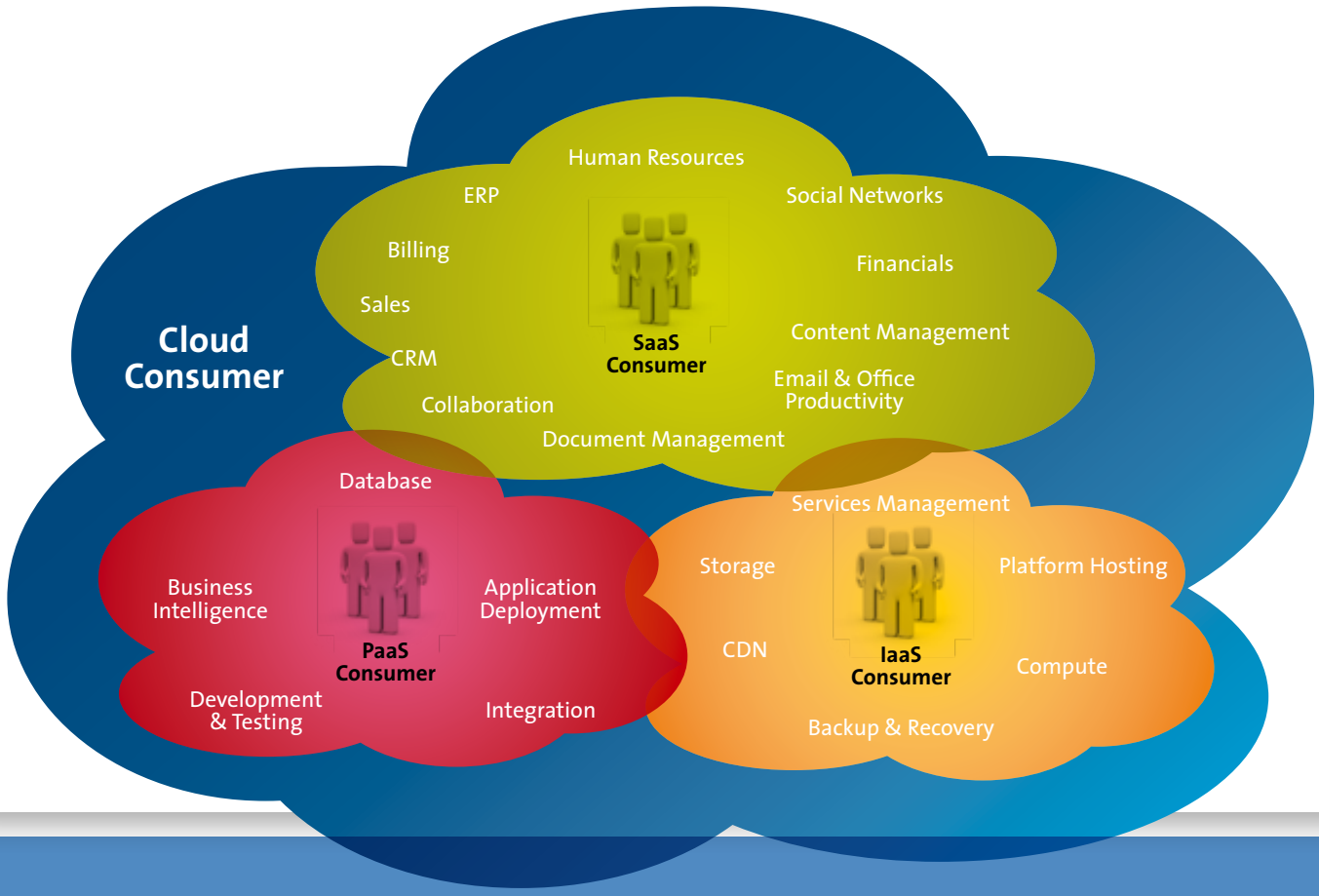
En el contexto del sector P*roductos de Consumo y Retail, Cloud Computing* contribuye a eficiencias en la recolección y análisis de grandes volúmenes de datos de ventas así como en la gestión de inventarios en tiempo real[4].

Los puntos de venta generan grandes cantidades de datos cada día. Los datos de ventas y patrones de consumo de los clientes se pueden obtener, por ejemplo, a través de tarjetas de fidelidad y cupones de descuento, y almacenarse en servidores del proveedor de servicios *Cloud* vía redes conectadas a las cajas registradoras. Las empresas pueden acceder a sus datos desde cualquier lugar vía Internet, permitiéndoles monitorizar el desempeño de sus productos, realizar análisis de los datos e identificar tendencias.

Para la gestión de inventarios, las empresas pueden almacenar en la nube en tiempo real datos sobre la venta de sus productos en numerosas tiendas, facilitando la información sobre la disponibilidad de los productos y la realización de pronósticos realistas a través del análisis de los datos.

En el resto de esta sección analizaremos las áreas de riesgo más importantes a las que habrá que hacer frente cuando se migra a *Cloud,* especialmente en relación a la seguridad de la información y la privacidad de los datos, y proporcionaremos un marco para guiar a las empresas en el proceso de migración.

Figura 1: Modelos de servicios en el Cloud de acuerdo al NIST (referencia 5) *



Servicios de *Cloud Computing* están disponibles a lo largo del espectro de servicios informáticos. El Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos ha definido tres modelos de servicios primarios[5]:

- **Infraestructura como servicio (IaaS):** Servicios de computación, almacenamiento y comunicación en red.
- **Plataforma como servicio (PaaS):** Bases de datos, herramientas de desarrollo y otros componentes necesarios para apoyar el desarrollo y despliegue de aplicaciones en la nube.
- **Software como servicio (SaaS):** Aplicaciones tanto a nivel general, por ejemplo procesamiento de texto, correo electrónico y hojas de cálculo, como especializadas, por ejemplo sistemas para la gestión de relaciones con clientes (CRM) y gestión de recursos empresariales (ERP).

**Las referencias a otras publicaciones se encuentran reunidas al final del documento.*

Adicionalmente, se definen cuatros tipos de despliegue de *Cloud Computing:*

- **Nube privada:** La infraestructura tecnológica es proporcionada para uso de una sola organización. La infraestructura puede pertenecer y ser gestionada por la organización misma, un tercero o una combinación de ambos; y pueden existir dentro o fuera de las instalaciones de la organización.

- **Nube pública:** La infraestructura tecnológica es propiedad de una organización que vende servicios en la nube, y está disponible para el uso del público en general.

- **Nube comunitaria:** La infraestructura tecnológica es compartida por varias organizaciones que tiene algún objetivo común (por ejemplo, una misma misión, requisitos de seguridad similares, o las mismas consideraciones de cumplimiento regulatorio). Puede ser administrado por una de las organizaciones o por un tercero.

- **Nube híbrida:** La infraestructura tecnológica es una composición de dos o más tipos de nubes (privada, comunitaria o pública).

2.1 Retos en la adopción de Cloud Computing

Como la mayoría de los cambios tecnológicos, implementar la tecnología *Cloud* requiere considerables cambios en los métodos tradicionales de gestión de la tecnología y en los procesos de negocio, creando nuevos retos para los CIOs, particularmente en relación con la seguridad y privacidad de datos. Estos retos han sido identificados por diversas organizaciones y grupos de trabajo, tales como Cloud Security Alliance (CSA)[6], National Institute of Standards and Technology (NIST)[7], European Network and Information Security Agency (ENISA)[8], o grupos de expertos convocados por la Comisión Europea[9], entre otros.

El modelo de negocio de *Cloud Computing* implica que los usuarios de servicios *Cloud* no pueden determinar exactamente dónde están ubicados sus datos, lo cual crea cierta inquietud entre los usuarios, y problemas de confianza entre los usuarios y los proveedores de los servicios.

Otra área que ha creado cierta inquietud es la privacidad de los datos. Por un lado, información personal almacenada en la nube requiere un tratamiento mucho más riguroso que si la información estuviese almacenada en equipos de la empresa, para evitar su acceso por terceros desde el interior de los centros de datos. Sin embargo, el núcleo del problema de privacidad para las empresas que adoptan *Cloud Computing* es la diversidad de normas de unos países a otros en relación a la privacidad, lo cual es especialmente inquietante en un modelo en el cual no se conoce la ubicación física de los datos.

Siguiendo el estudio Global Information Security Survey 2011 de Ernst & Young[10], a continuación presentamos las áreas de riesgo más importantes que hay que tener en cuenta cuando se migra a un modelo de *Cloud Computing*.

- **Seguridad de la información e integridad de los datos**. El procesamiento de datos a través de un proveedor de servicios *Cloud* requiere el envío de dichos datos vía Internet, frente a mantener los datos dentro de la red de la empresa, lo cual incrementa las vulnerabilidades de seguridad. Algunos de los riesgos de seguridad de la información más significativos cuando ésta es procesada en la nube son el acceso no autorizado a las áreas lógicas y físicas de la red, la modificación no autorizada de los sistemas o datos y la supresión no autorizada de datos. Una preocupación común de las empresas reside en perder el control de su información de negocio al confiar en los proveedores de *Cloud* la autenticación segura, las credenciales de los usuarios o la gestión de datos.

- **Privacidad y cumplimiento regulatorio.** En lo que respecta a la privacidad, una sola filtración de datos podría perjudicar significativamente el nombre de la organización, empañar su reputación y limitar su crecimiento en el futuro, además de los costes directos de dicha filtración. Las organizaciones están obligadas, por ley o norma de la industria, a almacenar, trazar e incluso no transferir cierta información. El movimiento de datos a la nube no exime a la organización de la responsabilidad por el cumplimiento normativo; todo lo contrario, independientemente del lugar donde residan los datos, la organización sigue siendo responsable de sus obligaciones. Como tal, la empresa tendrá que entender a fondo los requisitos legales y regulatorios en cada jurisdicción en la que la organización y el proveedor operen.

- **Estándares y operatividad.** Los proveedores de servicios *Cloud* suelen desarrollar servicios personalizados que satisfacen las necesidades deseadas de su público objetivo. Sin embargo, para interactuar de forma eficaz con las aplicaciones del proveedor, es vital que los sistemas de las compañías y las del proveedor puedan comunicarse entre sí. Si los sistemas no pueden hablar uno con el otro, la continuidad de los procesos, el rendimiento de la aplicación, la incapacidad para personalizar las aplicaciones y la eficiencia global de los servicios deseados están en riesgo. La estandarización está en desarrollo, pero es un largo proceso.

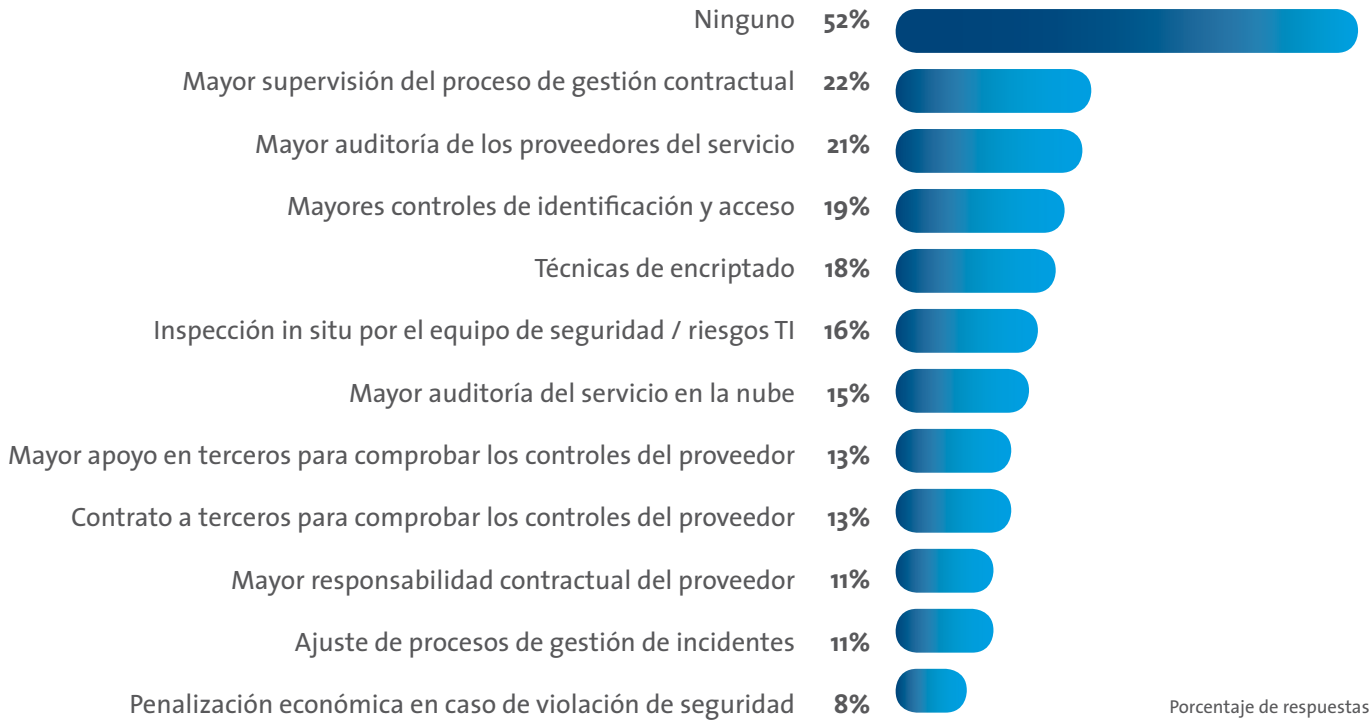
- **Gestión de proveedores y gobierno.** Los acuerdos de nivel de servicio o contratos a menudo estipulan la capacidad de un cliente para auditar a un proveedor, los recursos legales válidos cuando se produzcan incidentes y cuál de las partes es propietaria de los datos almacenados en la nube. Asimismo, a menudo contienen detalles cruciales relativos a los elementos clave de servicio, tales como el nivel o porcentaje de disponibilidad y espacio de almacenamiento asignado. Estos términos son a menudo no negociables, especialmente para los usuarios de las ofertas de servicios básicos.

2.2 Recomendaciones para el uso de la tecnología Cloud

La mayor parte de los controles de seguridad están basados en estándares como ISO 27001, adaptados para el modelo de *Cloud Computing*[11]. Sin embargo, de acuerdo con el estudio Global Information Security Survey 2011 de Ernst & Young, donde se encuestaron a cerca de 1.700 organizaciones de diferentes sectores en 52 países, incluyendo 104 organizaciones del sector *Productos de Consumo y Retail,* se detectó que el 52% de los encuestados no está implantando controles para mitigar los riesgos de adoptar la tecnología *Cloud,* así como que el principal control utilizado por los encuestados es simplemente una mayor supervisión del contrato con el proveedor del servicio *Cloud,* el cual lo lleva a cabo solamente un 22% de los encuestados, como se muestra en la figura 2.

En el contexto español, el Observatorio Nacional de las Telecomunicaciones y de la SI – ONTSI- ha realizado un reciente estudio sobre los retos y oportunidades de Cloud Computing[12], particularmente para las pymes españolas. Entre los resultados encontrados cabe destacar que entre 1.700 empresas encuestadas, el 42,5% conoce Cloud Computing; el principal motivo para adoptar Cloud es la mayor flexibilidad y escalabilidad que aporta la tecnología; tiempo y costes son los principales beneficios

Figure 2. ¿Cuáles de los siguientes controles han implementado para mitigar los nuevos o crecientes riesgos relacionados con el uso de la tecnología cloud?



percibidos; y 63,4% de las empresas usuarias de Cloud recomendaría el uso de la tecnología sin ningún tipo de dudas a empresas de características similares. En contraste, los encuestados manifiestan que la mayor preocupación que tienen las empresas es seguridad y confidencialidad.

Como parte del estudio realizado por IE Business School y Ernst & Young, realizamos un grupo de trabajo con representantes de 10 empresas líderes del sector Productos de Consumo y Retail en España. En relación con Cloud Computing, todos los participantes reconocen los beneficios de la tecnología Cloud. Entre las empresas que han implantado la tecnología, los modelos seleccionados han sido los modelos de nube privada o nube híbrida.

La gobernanza en la nube implica muchos de los retos en la adopción de Cloud Computing a través del desarrollo de procesos para la certificación de servicios, marcos de auditoría como los utilizados en la industria de servicios financieros, y el desarrollo de guías y marcos de referencia sobre cómo las empresas pueden migrar a la nube.

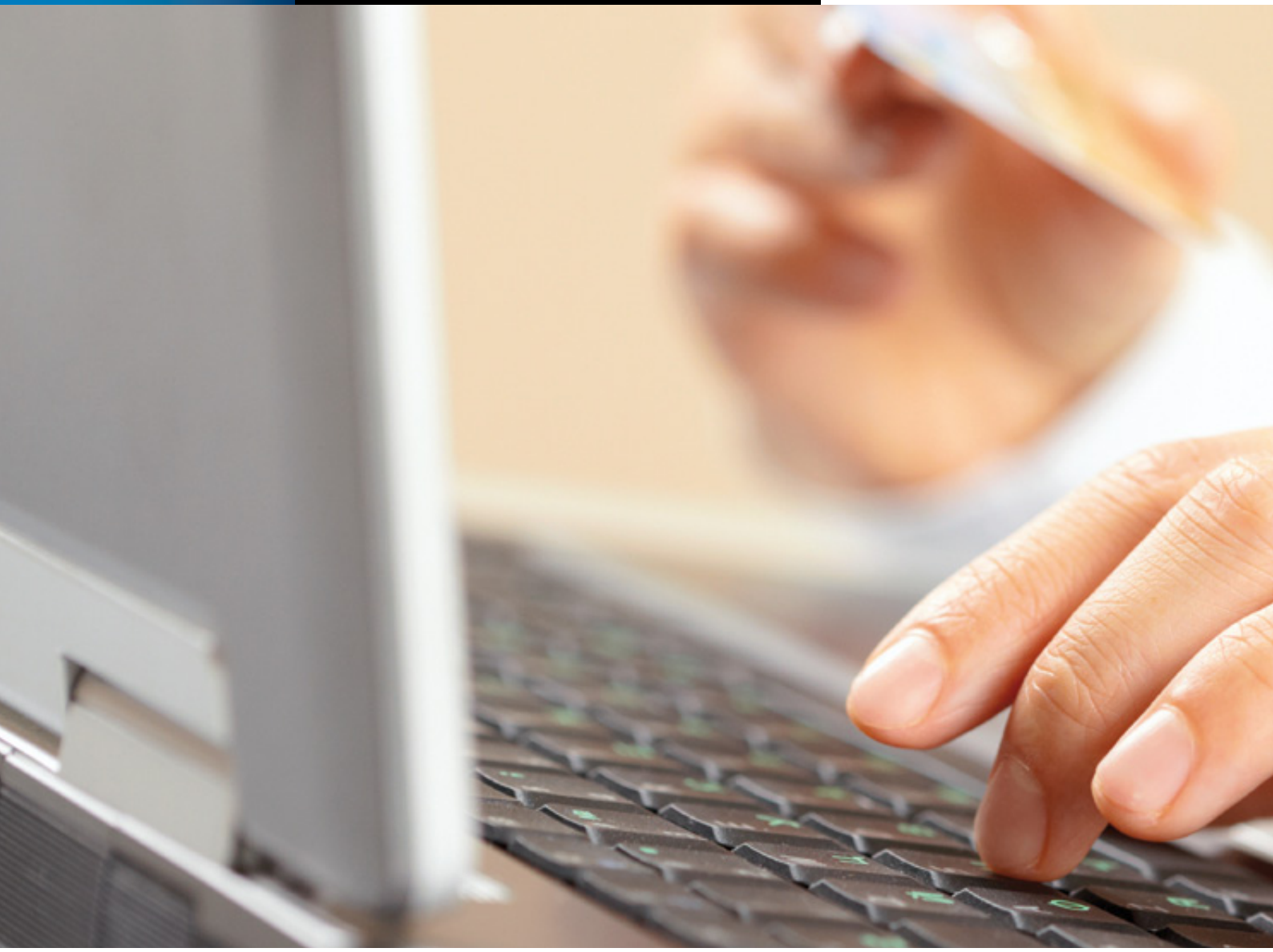
Ante los retos que presenta la adopción de Cloud Computing, varias organizaciones que impulsan el uso seguro y confiable de la tecnología Cloud, tales como ENISA en Europa o CSA y NIST en Estados Unidos, han comenzado a proponer controles para mitigar los posibles riesgos en la adopción de la tecnología y desarrollar el proceso de gobernanza en la nube[13].

A continuación presentamos un resumen de los pasos a seguir para evaluar la migración a Cloud Computing, de acuerdo con el marco de referencia propuesto por CSA:

- **Identificar los activos a migrar a la nube.** El primer paso en la evaluación de riesgo para el Cloud es determinar exactamente qué datos o aplicaciones van a migrarse a la nube.
- **Evaluar los activos.** El segundo paso consiste en evaluar los requerimientos de confidencialidad, integridad, disponibilidad y trazabilidad de los activos, buscando determinar cómo los riesgos cambian en caso de que los activos se encuentren en la nube.
- **Seleccionar el tipo de Nube apropiada,** ya sea pública, privada, híbrida o un modelo comunitario.
- **Seleccionar el modelo de servicio en la Nube,** ya sea aplicación, plataforma o infraestructura como servicio, y el proveedor de servicios Cloud.
- **Elaborar el posible flujo de datos** entre la organización, el servicio en la nube, y cualquier otro cliente/nodo.

A continuación presentamos nuestras recomendaciones en relación con la adopción de Cloud Computing en el sector Retail:

- **Ponga claridad en la gestión de los riesgos.** La empresa debe entender su propio grado de tolerancia al riesgo, así como quién corre con los riesgos antes de aceptar un contrato de Cloud. En particular, qué políticas sigue el proveedor ante violaciones de seguridad/privacidad, y qué acciones reparadoras sigue.
- **Elija la verificación por encima de la confianza.** Algunos de los interrogantes que deben considerar las empresas son si el proveedor de servicios Cloud está certificado de acuerdo a estándares internacionales, o si permiten auditorías externas sobre el procesamiento de los datos.
- **Elabore un plan de continuidad** y seleccione proveedores que sean transparentes con la creación de las copias de seguridad, los *backups* y las pruebas de recuperación del negocio ante fallos.
- **Proceda usando los procesos estándar de seguridad** y las técnicas que hayan funcionado de forma eficaz con otras tecnologías en el pasado.
- **Alinee su negocio y la estrategia de seguridad de la información,** y de forma continua evalúe los riesgos para cumplir con las regularizaciones y estándares de la industria.



Caso de estudio.
Fiabilidad ante la caída de un proveedor de servicios Cloud

La fiabilidad del Cloud ha sido un punto de discusión hasta el momento, con algunos comentando que no es tan fiable como una estructura local bien gestionada. Por ejemplo, en abril de 2011 una gran parte de la infraestructura de Web Services de Amazon falló durante tres días, dejando a muchas empresas que dependían del servicio sin acceso a sus aplicaciones y datos[14].

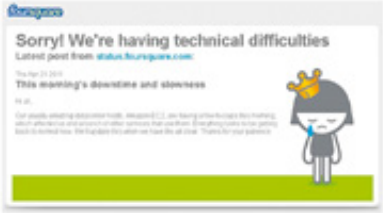
Figura 3. Noticia de la caída de Amazon Web Services en 2011 en BBC Mundo

Amazon se disculpa por la caída de su "nube"

Redacción
BBC Mundo
Sábado, 30 de abril de 2011

El gigante de las ventas en internet Amazon se ha visto obligado a pedir disculpas por un problema en su servicio de alojamiento de páginas web EC2 que sacó del aire a numerosos sitios.

El pasado jueves 21 de abril, la interrupción del servicio de Amazon hizo que se cayeran Foursquare, Reddit y Quora, algunos incluso más de un día.



Four Square fue uno de los sitios en internet que cayó por el fallo en los servidores de Amazon.

Sin embargo, otras empresas que utilizaban el servicio supieron salir adelante ante tal situación. Por ejemplo, Netflix, el servicio de suscripción de películas vía Internet, pudo seguir funcionando sin problemas. Netflix siguió recomendaciones de Amazon y diseñó una arquitectura que soportaba interrupciones en el servicio a través de replicación de datos y aplicaciones. Una parte importante del sistema de Netflix es una aplicación llamada Chaos Monkey[15], que permite finalizar automáticamente algunas aplicaciones y re-iniciar su funcionamiento en otros sitios. La falla de Amazon fue grave, pero afectó solamente a uno de sus centros de datos estadounidense. Con el uso de su Chaos Monkey, Netflix pudo manejar la interrupción del servicio en el centro de datos de Amazon sin problemas, y continuar prestando el servicio a partir de datos y aplicaciones almacenados en otros centros.

Lecciones del caso

El análisis sobre la fiabilidad de los proveedores de servicios Cloud, en conjunto, es del 99,9%[16]. Una fiabilidad bastante alta que seguramente es la envidia de muchos departamentos de TI que procesan sus datos de forma local. Debido a esta disponibilidad tan alta, cuando se producen caídas del servicio por parte de proveedores prominentes, reciben una importante atención de los medios.

Netflix ha gestionando muy bien los riesgos que trae el uso de la tecnología Cloud, y ha diseñado soluciones para mitigar tales riesgos. Una arquitectura con sistemas redundantes ha sido clave para continuar con el servicio ante caídas del proveedor.

3. Medios sociales en el sector *Productos*

A medida que la Web ha evolucionado, también lo ha hecho el mundo de las compras. Al comienzo, la Web era estática y sólo unos cuantos expertos podían crear contenido. En esas etapas iniciales, las Webs era simplemente un canal a través del cual las empresas promocionaban y vendían sus productos. Hoy día, la Web es social, con millones de personas utilizándola como su medio de comunicación, conversando con sus amigos y compartiendo experiencias.

Esta Web social presenta una gran oportunidad para las empresas. El valor de la economía basada en la Web para los países miembros del G20 se duplicará en el 2016, de acuerdo con el informe de enero del 2012 de Boston Consulting Group[17], el cual predice que dentro de cuatro años, aproximadamente, 3.000 millones de personas estarán utilizando Internet, cerca a la mitad de la población mundial. En relación con los medios sociales, diariamente un promedio de 172 millones de personas visitan Facebook, 40 millones visitan Twitter y 22 millones visitan LinkedIn. Más de 860.000 horas de vídeos se cargan diariamente en Internet y cerca de 35 millones de aplicaciones *(apps)* son descargadas.

Lo social puede ser utilizado por las empresas para crear una comunidad, captar nuevos seguidores de la marca e impulsar las ventas. Lo social abre un canal de comunicación directo entre la empresa y sus clientes, con ventajas para ambos. Los clientes empiezan a sentirse parte de la empresa y al ser parte de algo, es más probable que gasten su dinero en

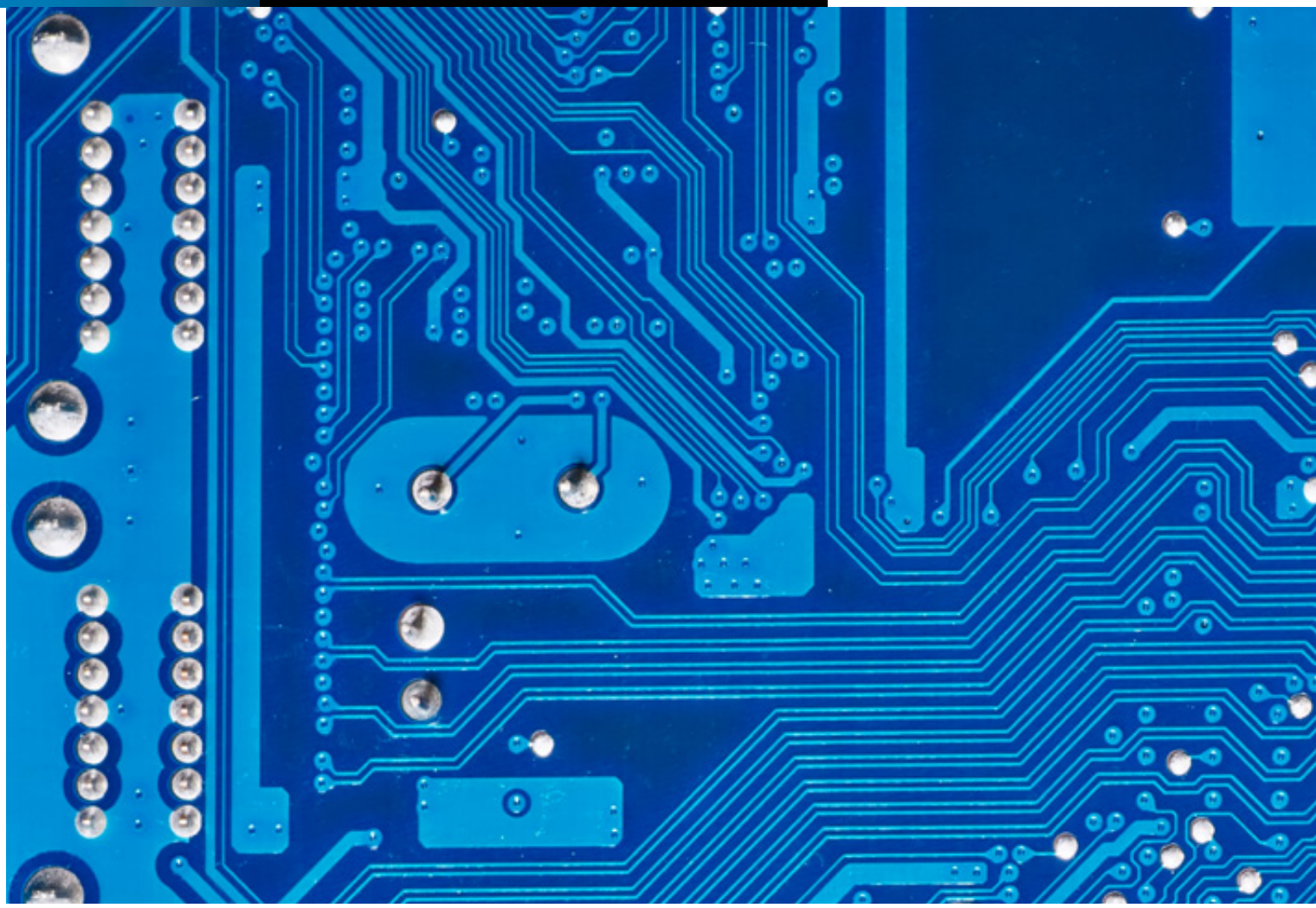
de Consumo y Retail

la empresa. Al escuchar a los clientes, las empresas pueden modificar sus ofertas y productos a fin de satisfacer los deseos de sus clientes, llevándolas a ser más propensas a vender.

Todo esto está teniendo un fuerte impacto en el sector. En un estudio sobre comercio social realizado por JWT Intelligence[18] se destaca el efecto de lo social en las compras. De acuerdo con el estudio, más del 40% de los hombres y más de un tercio de las mujeres son más propensas a comprar algo si un amigo se lo ha recomendado en una red social. En la misma línea, un estudio de Ernst & Young sobre los medios sociales en el Reino Unido en 2011[19] encontró que dos tercios de los encuestados consideran que los medios sociales van a influenciar sus decisiones de compra.

En el estudio realizado entre el IE y Ernst & Young, todas las empresas que participaron en el grupo de trabajo coinciden en la relevancia de los medios sociales para el sector, transformando la manera de comunicarse con los clientes.

Pero además de todas las oportunidades que los medios sociales generan, hay también muchos retos nuevos. En general, con los medios sociales está ocurriendo un fenómeno paralelo al de *Cloud Computing* y las tecnologías móviles, en el cual los límites de la empresa se van desvaneciendo y se presentan retos tales como la fuga inadvertida de información sensible de la empresa por la participación de los usuarios en los medios sociales o daños en la reputación de la organización por comentarios negativos de empleados o clientes.

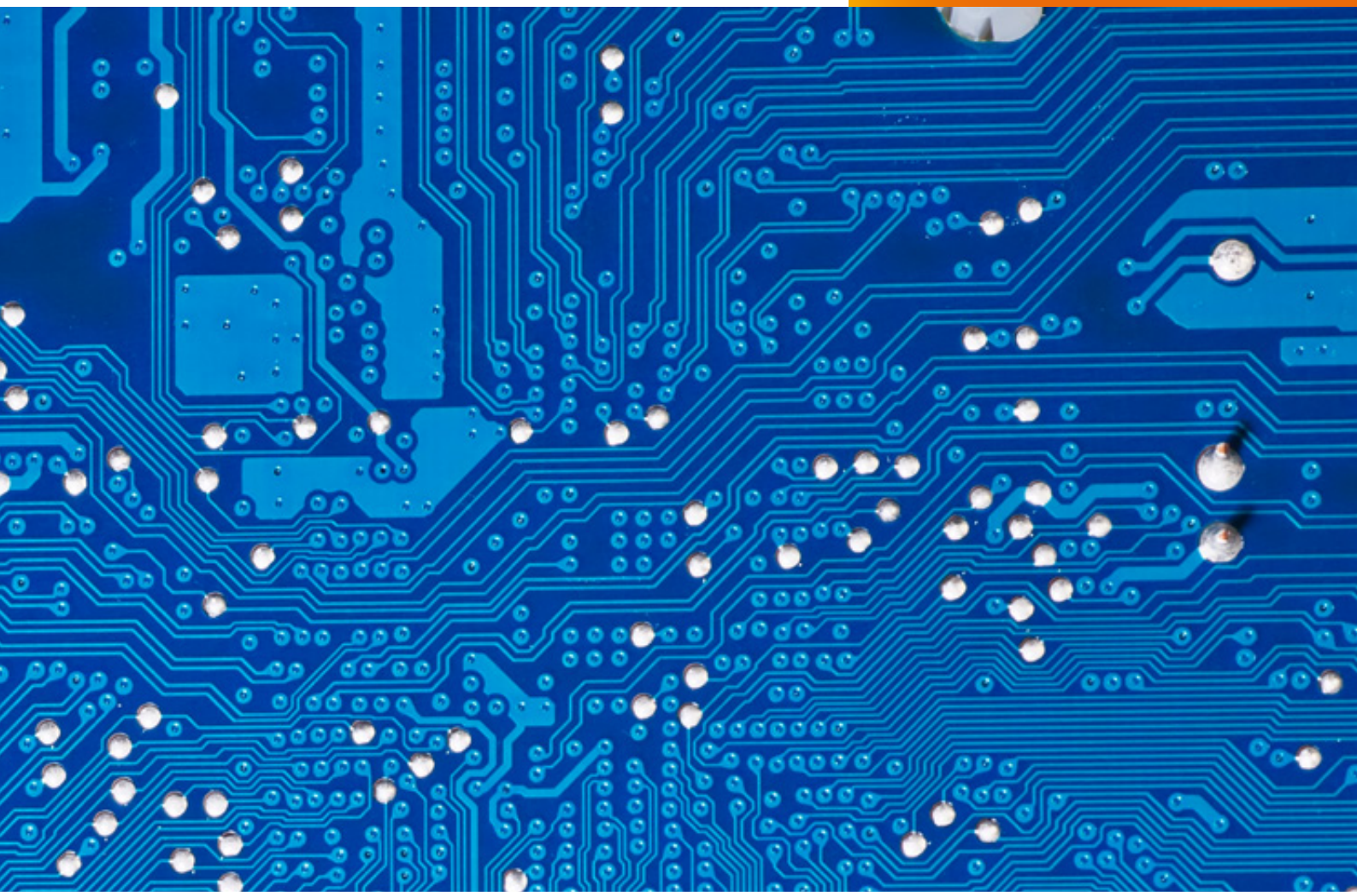


3.1 Entendiendo los riesgos de los medios sociales

Anteriormente, las empresas se basaban en datos transaccionales, tales como el historial de compras, para crearse una imagen de sus clientes y poder ofrecerles productos de acuerdo a sus necesidades. Con los medios sociales, las empresas tienen acceso a nuevos datos externos para incrementar la información sobre sus clientes y, por tanto, ofrecer productos mucho más personalizados.

Pero la transformación que se obtiene por los medios sociales implica cambios en la manera en que la empresa se acerca a sus clientes. Por un lado, se pasa de la transmisión -unidireccional- de la información a tener una conversación -bidireccional- con los clientes. Como resultado, las empresas tienen la oportunidad de conectarse con sus clientes de una nueva manera y crear nuevas relaciones.

Por otro lado, existe una responsabilidad por parte de las empresas hacia la información que fluye en los medios sociales. Las empresas no tienen control sobre la opinión de los consumidores, y puede que aparezca información que las empresas no consideran de uso generalizado o que afecte su reputación. Las organizaciones deben ser capaces de utilizar los medios sociales para participar en un diálogo con los clientes no satisfechos y críticos con el fin de corregir los errores y abordar las inquietudes de frente y de un modo público.



Tomando como partida el reciente estudio de Ernst & Young sobre protección y fortalecimiento de la marca[20], hemos identificados los siguientes riesgos relacionados con los medios sociales:

- **Riesgos reputacionales,** tales como daños a la reputación de la marca o de la compañía por publicaciones negativas por parte de empleados o clientes, incluso cuando son bien intencionadas.
- **Riesgos de seguridad.** Está teniendo un fuerte crecimiento el tipo de ataques de ingeniería social, con hackers criminales buscando obtener información confidencial (*logins* y contraseñas por ejemplo) a través de engaños. Por otra parte, estamos viendo un crecimiento en el número de virus y software malicioso para los medios sociales.
- **Riesgos de fuga de información.** Por ejemplo, empleados que participan en las redes sociales y, sin querer, filtran información confidencial de la empresa.
- **Riesgos operacionales.** Por ejemplo, empleados que hacen un uso indebido de las aplicaciones sociales en el trabajo.
- **Cumplimiento normativo.** Imposibilidad de retener y registrar la información de medios sociales en aquellos casos en que medidas regulatorias lo requieran.

Al participar en los medios sociales, se espera que la organización sea abierta y transparente. Las organizaciones que gestionan los riesgos ignorando comentarios de los clientes o restringiendo su participación en los medios sociales están cometiendo errores y los problemas pueden crecer de manera exponencial. Colaboración y aumento en la relevancia de los clientes son las nuevas monedas en la gestión de los medios sociales.

Algunas compañías responden a los retos de los medios sociales de forma rápida aportando soluciones parciales. Este enfoque a menudo resulta una pérdida de tiempo, energía y dinero, y provoca que las compañías tengan que reaccionar ante problemas que no estaban inicialmente previstos. Consideramos que las empresas deben construir una estrategia global holística para la gestión de los medios sociales, que abarque todos los esfuerzos en proteger y fortalecer la marca, y que sea lo suficientemente robusta y flexible como para acomodarse de forma constante a los distintos cambios que los avances tecnológicos producen.

Como base para nuestras recomendaciones para protección de la marca en los medios sociales hemos seleccionado como base el modelo responsabilidad digital desarrollado por Volovino y Robinson[21], el cual ha sido enriquecido con las recomendaciones de investigaciones previas de Ernst & Young[22]:

- **Desarrolle una estrategia de protección en los medios sociales que incluya el apoyo de la alta dirección.** Para que un programa de seguridad sea exitoso requiere el apoyo de la alta dirección. No es diferente para el caso de protección de la marca: es importante que los directivos entiendan por qué la organización está en los medios sociales y qué ventajas ofrece para el negocio. Es clave que miembros de la dirección muestren el compromiso de la organización con la estrategia, de manera que otros empleados se motiven e involucren en el proyecto.

- **Realice un análisis de riesgos del uso de los medios sociales.** Identifique claramente los potenciales riesgos. El análisis debe tener en cuenta la organización como un todo, así como el uso específico de los medios sociales por parte de los diferentes departamentos.

- **Defina políticas y guías de uso de los medios sociales.** Es importante tener en cuenta que las políticas estén de acuerdo con cualquier regulación existente, ya sea nacional o internacional. Un punto valioso es la realización de programas de concienciación sobre dichas políticas y guías, respondiendo al interrogante sobre el papel de los empleados en la estrategia de medios sociales.

- **Defina una estrategia para monitorizar los medios sociales,** incluyendo mecanismos para aprovechar los puntos de vista de los clientes y las lecciones aprendidas de monitorización.

- **Defina un proceso de respuestas a incidentes en los medios sociales,** teniendo en cuenta darle respuesta a las inquietudes de los clientes, así como aspectos de seguridad y privacidad de la información.

Caso de estudio.
Hacking en twitter de la cuenta del CEO

Best Buy es una de las empresas líderes en el mercado minorista de productos electrónicos, con más de 1.400 tiendas, más de 160.000 empleados, unos ingresos anuales cercano a los 50.000 millones de dólares, y considerado el décimo primer mayor sitio Web del sector Retail en los Estados Unidos[23].

Brian J. Dunn fue el CEO de Best Buy entre Abril de 2009 y Abril del 2012. Dunn es un convencido usuario de los medios sociales y sus ventajas para el negocio. Dunn utilizaba el blog corporativo, Twitter y Facebook como medios de comunicación para interactuar con clientes y empleados. En un artículo en Harvard Business Review[24] comenta: *"creo que el mensaje de Best Buy tiene que estar donde la gente está. Hoy día, significa estar en las redes sociales".*

En especial, Dunn era un ávido usuario de Twitter, con más de 5000 seguidores. En sus propias palabras *"Twitter es una forma de que la gente sepa lo que está en mi mente... Le comunico a mis empleados las cosas buenas que veo en una tienda o las buenas experiencias de los clientes. Los empleados están felices, saben que estoy escuchando buenas cosas sobre ellos".*

En 2010, los seguidores de Dunn en Twitter fueron sorprendidos por un mensaje inusual: *"I'VE BEEN HAVING A LOT OF GREAT SEX LATELY, AND HERE'S WHY",* seguido por una enlace a una página que ofrecía píldoras para aumentar el rendimiento sexual. Obviamente, su cuenta en Twitter había sido hackeada.

Dunn reconoció que, como mucha gente, estaba utilizando un password fácil de recordar, y de descubrir, basado en aspectos de su vida.

Figure 4. Cuenta de Dunn en Twitter como CEO de Best Buy

Lecciones del caso.

Con la ayuda del departamento de TI, Dunn reconfiguró su cuenta en Twitter, definió un password difícil de reconocer y que cambia con cierta periodicidad, siguiendo las políticas de la empresa.

Importante: la experiencia negativa no detuvo a Dunn para seguir utilizando los medios sociales, considerando que los aspectos positivos superan a los negativos. Él comenta que *"no se pueden utilizar [los medios sociales] sólo cuando las cosas van bien. Hay que enfrentarse tanto a la lluvia como al sol".*

4. Conectándonos en un mundo móvil

En las últimas décadas, hemos sido testigos de importantes avances tecnológicos en dispositivos móviles, desde los asistentes personales de datos (PDA) de finales de los 90 al uso difundido de smartphones y tabletas hoy día. Estos avances han ampliado las fronteras de la empresa, borrando los límites entre el hogar y la oficina, compañeros de trabajo y competidores. Por otro lado, el llamado m-commerce - comercio en móviles - está creciendo considerablemente. Por ejemplo, recientes estudios en el mercado norteamericano han mostrado que el 25% de los usuarios de móviles compra online usando un dispositivo móvil[25]. En el caso español, el reciente estudio de ONTSI[26] muestra que el 9% de los internautas ha realizado compras con dispositivos móviles. Estas cifras tienden a aumentar, a medida que los dispositivos móviles están teniendo una mayor acogida en la población.

A nivel empresarial, los dispositivos móviles permiten el acceso constante al correo electrónico y aplicaciones corporativas, lo que ha conllevado a reestructurar los modelos de negocio, el desarrollo de nuevas aplicaciones, y ha permitido el almacenamiento y acceso de datos empresariales, posiblemente confidenciales[27]. Estos cambios implican ciertos riesgos que las empresas deben tener en cuenta.

Adicionalmente, está ocurriendo otro gran cambio en las organizaciones. Un gran número de empresas están ofreciendo soporte técnico y acceso a sus aplicaciones desde dispositivos que pertenecen a sus empleados, el llamado *"bring your own device"* -BYOD[28], lo cual puede traer nuevos riesgos. Por ejemplo, un empleado puede, sin saberlo, reducir la seguridad de su propio dispositivo móvil abriendo las puertas a posibles ataques.

En otras palabras, un mayor acceso a la información ha conllevado una mayor productividad, pero también ha incrementado los riesgos de seguridad de la información. Las empresas tienen, por lo tanto, la necesidad de identificar los riesgos potenciales, desarrollar estrategias eficaces y aplicar medidas para hacer frente a estos riesgos.

En el sector *Productos de Consumo y Retail,* los consumidores se están aprovechando de la gran cantidad de canales y dispositivos que les permiten realizar sus compras en cualquier momento, en cualquier lugar y más rápido que nunca, evidenciado por el creciente número de aplicaciones para smartphones que agilizan, y hacen más sencilla, las compras. El ritmo de cambio en los próximos años va a ser rápido, y el sector debe estar preparado para responder a las expectativas de los consumidores y su deseo de un comercio más rápido, más cómodo, y más personalizado.

4.1 Riesgos en el uso de dispositivos móviles

La ubicuidad de los dispositivos móviles en el entorno empresarial ha permitido una mayor expansión de la oficina corporativa. Desde una perspectiva de seguridad, los riesgos y los posibles efectos del despliegue y soporte de dispositivos móviles como herramienta corporativa deben ser entendidos. A continuación presentamos los principales riesgos en relación con los dispositivos móviles, de acuerdo a estudios sobre seguridad en dispositivos móviles de Ernst & Young[29] y SearchSecurity.com[30].

- **Dispositivos robados o extraviados.** Un problema fundamental de los dispositivos móviles es el control de acceso físico. Por su diseño, los dispositivos móviles son más útiles fuera de la oficina y en movimiento con el propietario. Esto presenta varios desafíos para un administrador de seguridad, ya que un dispositivo en movimiento es más probable que se pierda o sea robado, y posteriormente utilizado por un atacante malintencionado.

- **Administración del dispositivo por parte de los usuarios.** En comparación con los ordenadores portátiles, los dispositivos móviles a menudo contienen más controles en el lado cliente que pueden ser alterados, lo que puede causar problemas de seguridad. Por ejemplo, en ocasiones es posible cambiar la política de bloqueo del terminal o utilizarlo como *modem*. Esto puede eludir ciertas restricciones de dispositivo y permitir a un usuario malicioso atacar la red interna más fácilmente. Adicionalmente, los propietarios pueden evitar las restricciones de los dispositivos a través de un método conocido como *"jailbreaking"*, pudiendo eliminar todos los requisitos de política sobre el dispositivo, instalar aplicaciones no aprobadas y exponerse a potenciales amenazas de seguridad adicionales.

- **Software malicioso vía aplicaciones**. El principal método de funcionamiento para acceder a software y datos corporativos desde dispositivos móviles es vía aplicaciones, que se pueden adquirir a través de diversas tiendas de aplicaciones o ser proporcionadas por la empresa. Un riesgo es la instalación de software malicioso como aplicaciones para el dispositivo. Recientemente, tiendas de aplicaciones como Google Play han tenido que incrementar su proceso de selección de aplicaciones ante un incremento en el número de aplicaciones maliciosas[31].

4.2 Recomendaciones para la seguridad en dispositivos móviles

A continuación presentamos una serie de recomendaciones para utilizar dispositivos móviles en las organizaciones de forma segura, basadas en recomendaciones presentadas en otros estudios [32, 33]

- **Crear e implantar políticas de TI que regulen el uso de dispositivos móviles.** Las políticas deben incluir cómo mantener la información privada y definir la propiedad de los datos y aplicaciones en los dispositivos corporativos. Establecer programas de divulgación para que las políticas sean conocidas y entendidas por todos los empleados.

- **Implantar seguridad a nivel de dispositivos móviles.** Todos los dispositivos móviles deben estar protegidos con password; así mismo se debe limitar los datos sensibles transferidos a los dispositivos, o considerar su acceso de sólo lectura. Es importante evaluar utilizar un software de gestión de dispositivos móviles que garantice una conexión cifrada en caso de acceder a datos sensibles. Adicionalmente, se recomienda formar a los desarrolladores de aplicaciones en prácticas de codificación seguras para plataformas de dispositivos móviles.

- **Creación de un grupo de trabajo sobre seguridad en dispositivos móviles.** Entre las tareas del grupo se debe realizar evaluaciones técnicas sobre la seguridad en los dispositivos móviles y en la infraestructura de apoyo; así como evaluar amenazas nuevas que aparezcan. Adicionalmente, se recomienda incluir seguridad de dispositivos móviles en los programas existentes de sensibilización de los empleados en el tema de seguridad.

Caso de estudio.
Cuando una aplicación gratuita sale costosa

Una cadena de almacenes de productos alimenticios fue víctima de una violación de seguridad. La gravedad de la violación se manifestó por el hecho de que la cadena no tenía ni idea de lo que había ocurrido. Sólo cuando la unidad de crímenes digitales de la policía llegó a visitar una de las tiendas, la empresa se enteró de que había sucedió un ataque de seguridad.
El fraude fue descubierto cuando sucursales de bancos en diferentes partes del país comenzaron a recibir llamadas de clientes que se quejaban de compras no realizadas y cargadas a sus tarjetas de crédito. Los bancos alertaron a la policía y la evidencia parecía indicar que algún tipo de captura de información se llevaba a cabo cuando se realizaban transacciones con tarjetas de créditos en varias tiendas de la cadena.

La reacción inicial de los directivos fue pensar que el fraude debía venir de otra parte, ya que la empresa seguía los estándares establecidos por la industria para el manejo de pagos con tarjetas de crédito. De todos modos, la empresa cooperó con la policía para que realizara las investigaciones del caso.

Personal de la policía inspeccionó los registros de transacciones de varias tiendas, y encontró un software malicioso instalado en el sistema que gestionaba la información en los puntos de venta. El software era un analizador de paquetes[34] que "miraba" los datos que salían desde los puntos de venta, y capturaba la información de tarjetas de crédito antes de que se eliminara de los puntos de venta y servidores de la empresa, lo que, de acuerdo a los estándares de la industria, debe ocurrir inmediatamente después de recibir la autorización del banco. Debido a que el software malicioso era un código personalizado, detectores de virus y software similares de prevención nunca lo habían detectado. Para gran sorpresa de la empresa, el software se encontró en cada una de las tiendas de la cadena.

Pero, ¿cómo llegó a instalarse el software malicioso en los sistemas de la empresa? Al realizarse un análisis forense, los registros de acceso mostraron que el software se había instalado inmediatamente después de que algunos usuarios accedieran a transacciones empresariales desde dispositivos móviles. La empresa había realizado una actualización de su sistema ERP hacía un año; la actualización permitía el acceso a los sistemas corporativos desde dispositivos móviles. Aunque no se permitió acceso móvil a los usuarios en general, algunos directivos lo solicitaron y el departamento de TI les dio acceso, de manera excepcional, tanto desde dispositivos corporativos como personales. Al revisar los dispositivos, se descubrió que uno de los directivos tenía instalado una versión gratuita, y no legítima, de un conocido juego. Dicha aplicación era utilizada por hackers para entrar en los equipos a los que se conectaba el usuario e instalar el software malicioso.

Lecciones del caso

Varias lecciones pueden concluirse del caso. En primer lugar, la empresa creyó que al seguir estándares de la industria para la gestión de pagos con tarjeta de crédito estaba garantizando la seguridad de sus sistemas de pago. Estándares de la industria como PCI-DSS son una muy buena manera de mostrar que la empresa sigue una gestión de calidad en el manejo de la información, pero no garantizan la seguridad de los activos del negocio[35].

Obviamente, BYOD trae ventajas para la empresa, a pesar de potenciales riesgos de seguridad[36]. La empresa debió definir políticas claras para el manejo de dispositivos móviles, buscar maneras de garantizar la seguridad de todos los dispositivos móviles de sus usuarios y, de vital importancia, realizar programas de concienciación sobre el uso seguro de los mismos.

Fuga de datos

Durante los últimos años, compañías de todo el mundo de diversos sectores de la industria han visto cómo sus datos más delicados se perdían, los robaban o se filtraban al mundo exterior. Una amplia variedad de incidentes de pérdidas de datos con información relevante han supuesto un elevado coste, de forma directa e indirecta, provocando grandes daños a las compañías, las marcas y su reputación.

Diferentes tipos de incidentes han ocurrido, incluyendo la venta de datos de clientes a empresas de terceros y la pérdida de muchos portátiles, memorias USB, cintas de backup y dispositivos móviles, por nombrar algunos. La inmensa mayoría de estos incidentes han sido resultado de acciones realizadas por usuarios internos y empresas externas de confianza, y en la mayoría de casos de forma involuntaria.

Como los datos son uno de los bienes más preciados de una empresa, protegerlos y mantenerlos fuera del dominio público es de vital importancia. Una de las técnicas para lograr tal fin es DLP (abreviatura de "Data Loss Prevention", prevención de fuga de datos en inglés), un conjunto de productos y estrategias que ayudan a las empresas a proteger la información[37]. DLP no es un producto independiente como por ejemplo un firewall, consiste de un grupo de tecnologías que permite prevenir la pérdida de datos mediante la identificación de los datos sensibles, seguimiento de su actividad, y bloqueo de los datos cuando se mueven de un sitio a otro, en caso de violar reglas preestablecidas.

Sin embargo, antes de que los controles DLP puedan implementarse de forma eficaz, una empresa debe entender las respuestas a tres preguntas fundamentales:

- ¿Qué datos sensibles mantiene la empresa?
- ¿Dónde se almacenan los datos sensibles, tanto internamente como en empresas de terceros?
- ¿Cuál es el destino y el flujo de los datos en la organización?

5.1 Retos en la gestión de la fuga de datos

La información derivada de los datos es la baza de mayor valor de cualquier organización. Un gran número de filtraciones de información de gran importancia han traído de nuevo a la actualidad este problema.

Con las recientes incorporaciones de la tecnología *Cloud*, el riesgo de la pérdida de datos ha crecido rápidamente. El incremento de la cantidad de datos que se llevan de un lado para otro con el uso de los dispositivos móviles ha aumentado el riesgo de que terceras partes puedan obtener acceso a información de carácter confidencial.

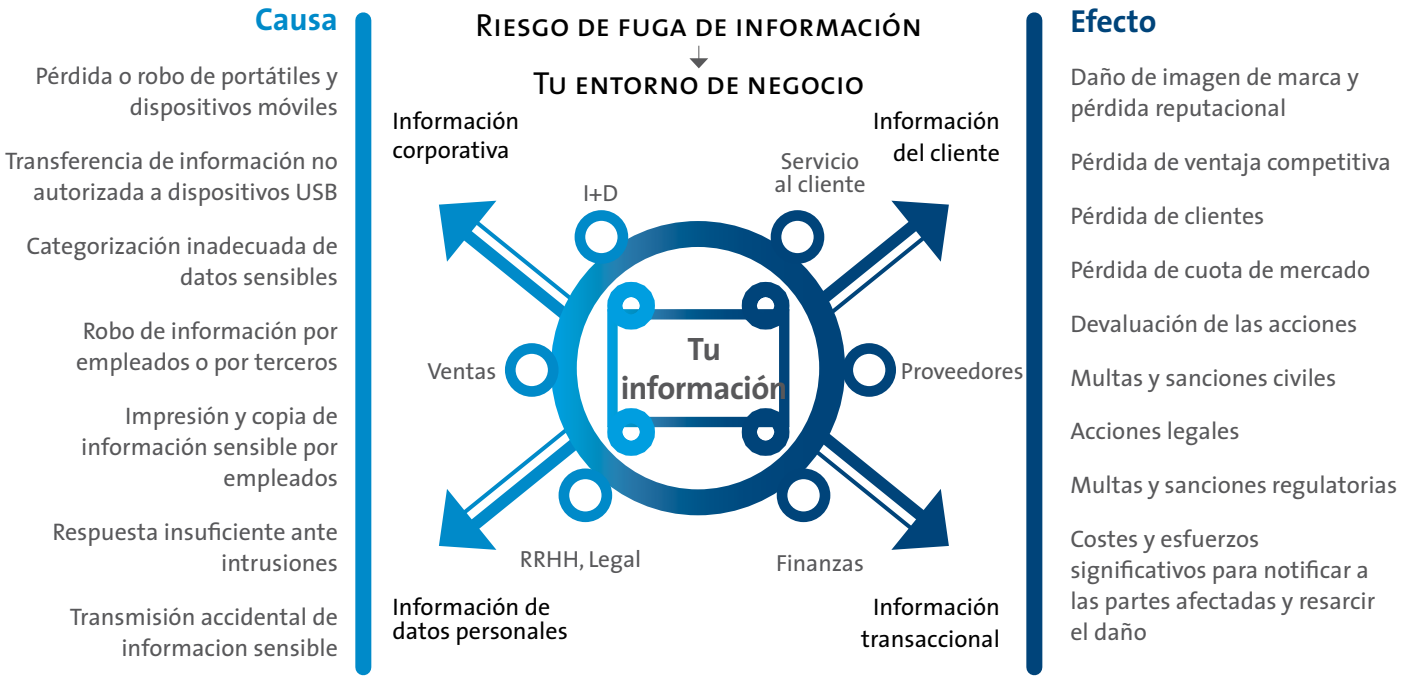
Pero la pérdida de datos no se limita sólo al riesgo de la pérdida física de los dispositivos como tabletas, teléfonos móviles o portátiles. Muchos incidentes son también debidos a la divulgación accidental a través de las transmisiones electrónicas o en los medios sociales. En la mayoría de los casos, los empleados no son conscientes de los riesgos asociados que los datos delicados a través de emails no cifrados, mensajes instantáneos, correo Web y herramientas de transferencia de datos.

Las fisuras que permiten la fuga de datos crecen debido al uso de sistemas descentralizados y herramientas colaborativas de trabajo, haciendo aun más difícil para las organizaciones trazar y controlar la información.

Otro factor que complica el control de los datos es la disponibilidad creciente de medios de almacenamiento de bajo coste. Muchos *gigabytes* de datos pueden literalmente "salir andando" por la puerta en la memoria USB de un empleado o en un *smartphone,* o pueden ser interceptados a través de un servicio de *Cloud* de bajo coste.

En la gestión de la fuga de datos hay muchas razones por las que la pérdida de datos pueda ocurrir, numerosos escenarios de pérdida de datos para tener en cuenta y muchos controles diferentes que deben ser eficaces con el fin de manejar el problema[38]. El problema se debe afrontar a través de una solución integral que incluya personas, procesos y necesidades tecnológicas a implementar, como se ilustra en la figura 5.

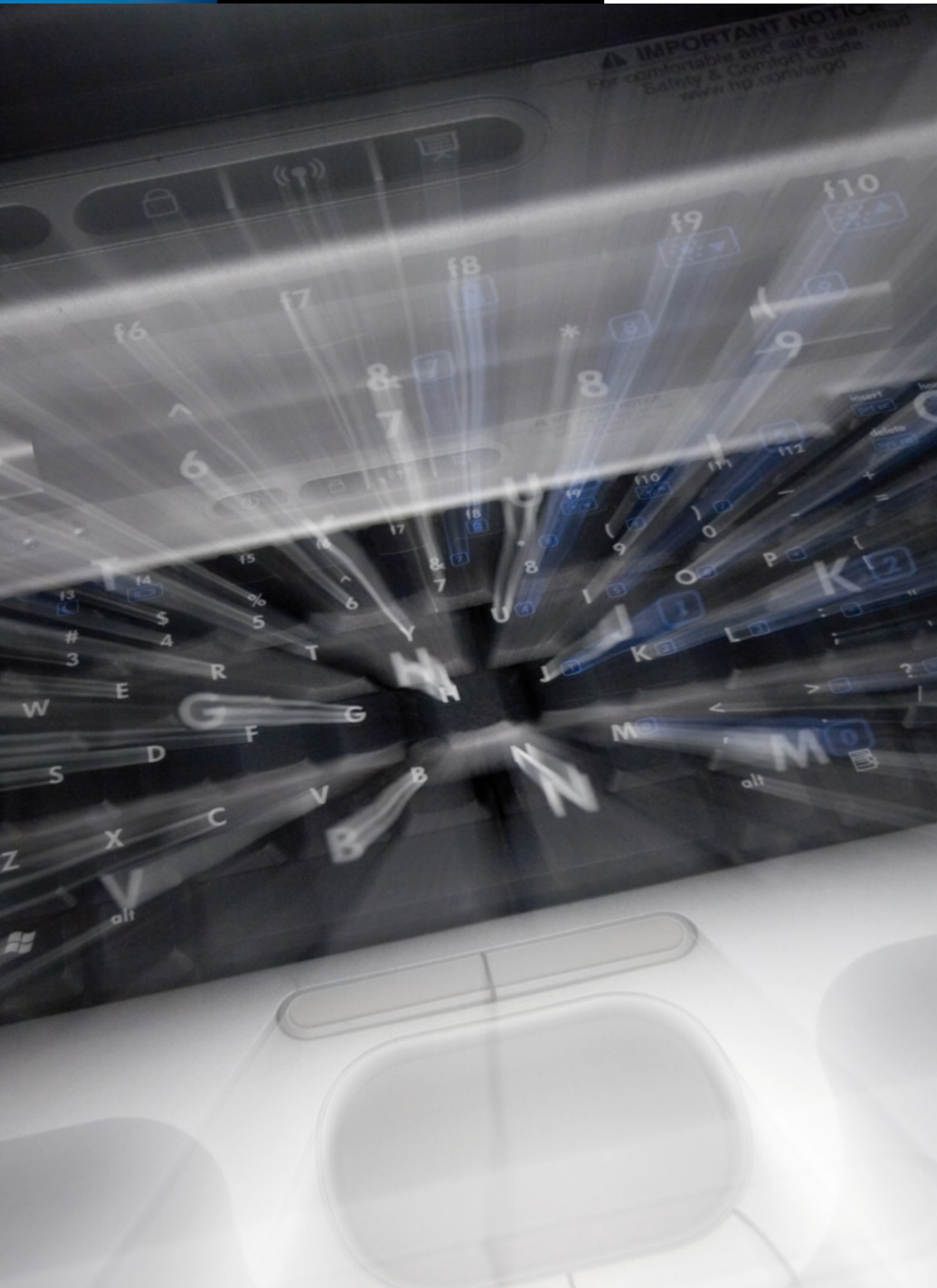
Figura 5: Causas y efectos de la fuga de datos en el ambiente empresarial. Adaptado del informe de Ernst & Young sobre fuga de datos (referencia 39).



5.2 Recomendaciones para la gestión de la fuga de datos

A continuación presentamos algunas recomendaciones para la gestión de la fuga de datos, basados en estudios previos[40],[41]:

- **Identifique, evalúe y clasifique los datos sensibles** a lo largo de la empresa de modo que los controles de prevención de fuga de datos puedan centrarse en proveer protección para los datos más sensibles y de mayor importancia para la empresa.
- Evalúe, comprenda y aprecie los riesgos potenciales y áreas de fuga de datos, específicamente **documentando y clasificando los riesgos relativos a los canales de fuga de información** que existen en la compañía.
- **Identifique controles claves de la prevención de fuga de datos y cuantifique su eficacia.** Todos los controles clave que soportan un programa de prevención de fuga de datos, tales como la gestión de activos y los controles de seguridad físicos, deben ser comprendidos para proporcionar reportes precisos de los riesgos y controles de la pérdida de datos.
- **Entienda qué datos se envían a terceras partes, cómo se envían y si los mecanismos de envío son seguros.** Las organizaciones tienen la responsabilidad de realizar la debida diligencia para validar que los administradores de terceras partes tienen medidas de seguridad razonables para proteger los datos sensibles de la compañía.
- **Proteja los datos en movimiento,** tanto los datos sin uso como los que se encuentran en uso dentro de los controles de prevención de fuga de datos de la organización.
- **Establezca un programa de respuesta a incidentes,** en el que incluya personal capacitado e involucre a las principales partes interesadas en el negocio.


IMPORTANT NOTICE
For comfortable and safe use, read
Safety & Comfort Guide
www.hp.com/ergo

Caso de estudio.
Robo de Datos en TJX

TJX fue el mayor minorista de prendas de vestir y productos para el hogar en los Estados Unidos en el segmento "off-price". Para el año 2006, TJX ocupaba el puesto 138 en el ranking Fortune 500; con unas ventas de 17.400 millones de dólares en los Estados Unidos para el ejercicio fiscal finalizado enero de 2007, la compañía era el triple del tamaño de Ross Stores Inc., su competidor más cercano.

Fue el 18 de diciembre de 2006 cuando TJX tuvo conocimiento de una intrusión en sus sistemas. La presencia de software sospechoso, así como archivos y datos alterados en los ordenadores de la empresa, fueron la primera evidencia de la intrusión en la red informática que gestionaba los pagos con tarjetas de crédito, cheques y devolución de mercancía. Parecía afectar a los ocho negocios de la compañía y todas sus tiendas en los Estados Unidos, Puerto Rico, Canadá y Reino Unido.

Para marzo de 2007[42], TJX anunció que 45,6 millones de números de tarjetas de crédito y débito fueron robados de uno de sus sistemas durante un período de más de 18 meses por un número desconocido de intrusos. Adicionalmente, fueron robados los datos personales facilitados en relación con la devolución de mercancía de cerca de 451.000 personas en el año 2003 también fue robado. En octubre[43], el número de tarjetas afectadas se duplicó a cerca de 94 millones y las pérdidas para los bancos estaban estimadas entre 68 y 83 millones de dólares.

Pero, ¿cómo sucedió realmente la intrusión en TJX? Expertos en TI consideran que, dada la magnitud de la intrusión, ésta se debió realizar desde diversos puntos. Las investigaciones reportaron que la empresa utilizó técnicas de cifrado débiles que permitieron a los intrusos descifrar la información. The Wall Street Journal[44] informó de que el ataque empezó en 2005 a través de la red "wireless" de una de las tiendas Marshall de TJX. Por otra parte, Information Week[45] consideró que otro medio de ataque fue vía ingeniería social, con algunos de los participantes fingiendo solicitar trabajo en TJX y logrando tener acceso a los equipos de los departamentos de selección, desde donde instalaron software malicioso que tenían en memorias USB.

Lecciones del caso

Las pérdidas tanto económicas como en reputación para TJX han sido grandísimas. Un año después del robo de datos, los costes en los que la compañía incurrió asciendieron a 250 millones de dólares[46].

Las investigaciones mostraron que la empresa almacenaba datos de los clientes que no necesitaba, como la información que se encuentra en las bandas magnéticas de las tarjetas de crédito. Para dicha información, TJX no tenía establecido controles para evitar su fuga. Adicionalmente, la empresa no había establecido controles de seguridad de acuerdo a estándares de la industria, tales como el "Payment Card Industry Data Security Standard" (PCI en sus siglas en inglés).

El caso muestra que la empresa tuvo un camino que recorrer, cambiando su acercamiento a la seguridad de sus sistemas de información. Un camino inicial para TJX fue una revisión de los principales riesgos que tenía y establecer estrategias para mitigarlos, de manera que una intrusión como la ocurrida no se volviera a repetir. En el mediano plazo, la seguridad de la información tiene que ser vista como algo no solamente técnico, sino que impacta fuertemente en el negocio y requiere la participación de todo el personal de la empresa.

6. Viewpoint de Ernst & Young

La historia de Amanda presentada en la introducción, es ficticia, pero las situaciones descritas y las interacciones de los clientes de las empresas de *Productos de Consumo y Retail con Cloud Computing*, los medios sociales y los dispositivos móviles son ya una realidad. Asimismo, como consecuencia de estas nuevas tecnologías las empresas están aumentando la exposición al riesgo frente a la fuga de información corporativa sensible.

Los beneficios que aporta el *Cloud Computing*, la necesidad de estar presente en los medios sociales y las ventajas de la utilización de los dispositivos móviles afectan a todos los sectores, pero quizás las empresas de *Productos de Consumo y Retail*, son las que más se sienten presionadas a adoptar estos cambios para no quedarse rezagadas respecto a sus competidores.

La mayoría de las compañías del sector, para seguir manteniendo la competitividad, tienen encima de la mesa los temas desarrollados en el presente estudio, o bien porque están inmersos en un cambio o porque tienen en mente realizarlo en un futuro inmediato.

Muchas de estas compañías se encuentran ante la incertidumbre de cómo abordar tecnológicamente estos cambios de comportamiento social desde el punto de vista de la seguridad. Necesitan saber a qué nuevos riesgos se están exponiendo, y con el fin de mitigarlos, cómo deben afrontar los cambios que están sufriendo sus modelos de negocio.

En el presente informe hemos querido profundizar en los procesos que encontramos día a día con clientes del sector decididos a abordar los retos tecnológicos con el nivel de seguridad que requieren y aprovechar las oportunidades de negocio que las nuevas tendencias les brindan.

RAMIRO MIRONES GÓMEZ

Socio de Ernst & Young

Cuenta con 14 años de experiencia en Ernst & Young realizando Auditorías de Sistemas de Información, así como proyectos de asesoría para la adaptación a los requisitos de seguridad informática y control interno. Además ha participado en auditorías relacionadas con la ley Sarbanes Oxley, sección 404.

Dentro del departamento de IT Risk and Assurance Services (ITRA), es el responsable del sector de Productos de Consumo y Retail así como de Telecomunicaciones, incluyendo entre sus clientes las más importantes compañías de España y Estados Unidos. También es el responsable del Centro de Competencias ERP en España.

Ramiro es Licenciado en Administración y Dirección de Empresas por la Universidad de Valladolid, Licenciado con Honores en Económicas y Estadística con Estudios Europeos por la Universidad de Exeter y Executive MBA por IESE Business School.

Referencias

1 D. Rigby. The Future of Shopping. Harvard Business Review, Vol 89, Issue 12, December 2011

2 CompTIA. Retail Sector Technology Adoption Trends Study. compTIA, the IT Industry Association. Junio 2012.

3 M. Armbrust, et al. Above the Cloud: A View of Cloud Computing. Communication of the ACM 53 (4), 50-58, 2010.

4 Fibre2fashion.com. The Future of Retail Industry is in Cloud Computing. Agosto 20, 2010. http://www.fibre2fashion.com/industry-article/29/2883/the-future-of-retail-industry1.asp

5 F. Liu et al. NIST Cloud Computing Reference Architecture. NIST Special Publication 500-292. September 2011.

6 CSA. Top Threats to Cloud Computing V1.0. Cloud Security Alliance, March 2010. Disponible en https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

7 NIST. Guidelines on Security and Privacy in Public Cloud Computing. NIST, December 2011. Disponible en http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909494.

8 ENISA. Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información. ENISA 2009. Disponible en http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/view.

9 EU. The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond 2010, European Commission, 27 January 2010.

10 Ernst & Young. Into the cloud, out of the fog. Insights on IT risk. Business briefing, November 2011.

11 K. Julisch, M. Hall. Security and Controls in the Cloud. Information Security Journal, A Global Perspective. Volume 19, Issue 6, 2010.

12 ONTSI. Cloud Computing – Retos y Oportunidades. Observatorio Nacional de las Telecomunicaciones y de la SI – ONTSI. Mayo 2012. Disponible en http://www.ontsi.red.es/ontsi/es/estudios-informes/cloud-computing-retos-y-oportunidades.

13 Security Guidance for Critical Areas of Focus in Cloud Computing. V3.0. Cloud Security Alliance, 2011.

14 Amazon. Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region. http://aws.amazon.com/message/65648/.

15 K. Finley. Chaos Monkey: How Netflix Uses Random Failure to Ensure Success. December 2010. http://readwrite.com/2010/12/20/chaos-monkey-how-netflix-uses.

16 M. Gagnaire et al. Downtime statistics of current cloud solutions. IWGCR: The International Working Group on Cloud Computing Resiliency, 2012. http://iwgcr.org/wp-content/uploads/2012/06/IWGCR-Paris.Ranking-002-en.pdf.

17 Boston Consulting Group. The Internet Economy in the G-20: The $4.2 Trillion Growth Opportunity. 2012.

18 JWT Intelligence. Social Commerce. July 2011

19 Ernst & Young. YouGov Social Media Survey. 2011.

20 Ernst & Young. Protecting and strengthening your brand. Insights on IT risk, Business briefing. May 2012.

21 L. Volovino and S. R. Robinson. Principles and Practice of Information Security. Pearson Prentice Hall, 2004.

22 Ernst & Young. Op cit 20. Protecting and strengthening your brand.

23 About Best Buy. http://pr.bby.com/about-best-buy/

24 B. J. Dunn. How I Did It ... Best Buy's CEO on Learning to Love Social Media. Harvard Business Review, December 2010.

25 C. Tode. 25pc of mobile users shop online only via a smartphone or tablet. Luxury Daily, July 9 2012. http://www.luxurydaily.com/25pc-of-mobile-users-shop-online-only-via-a-smartphone-or-tablet-study/.

26 ONTSI. Comercio Electrónico B2C 2011. Observatorio Nacional de las Telecomunicaciones y de la SI –ONTSI. Octubre 2012. http://www.ontsi.red.es/ontsi/es/estudios-informes/estudio-b2c-2011-edici%C3%B3n-2012.

27 M. Satyanarayanan. Mobile Computing: The Next Decade. Proceedings of the ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond (MCS), ACM, 2010

28 T. Bradley. Pros and Cons of Bringing Your Own Device to Work. PC World, December 20 2011. Disponible en http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html .

29 Ernst & Young. Mobile device security. Insights on IT risk. Technical briefing, January 2012.

30 SearchSecurity.com. Enterprise Mobile Security Survey 2012. http://searchsecurity.techtarget.com/guides/Survey-Enterprise-mobile-device-security-2012.

31 BBC News. Android hit by rogue app malware. March 2011. http://www.bbc.co.uk/news/technology-12633923.

32 Ernst & Young. Op. cit 29. Mobile device security.

33 Webroot. Mobile Security Decision-Makers Report BYOD Threats Have Infiltrated Their Organizations

November 2012. http://www.darkreading.com/mobile-security/167901113/security/news/240124947/mobile-security-decision-makers-report-byod-threats-have-infiltrated-their-organizations.html

34 T. Bradley. Introduction to Packet Sniffing. http://netsecurity.about.com/cs/hackertools/a/aa121403.htm.

35 Infosecurity. PCI-DSS compliance does not always gurarantee security. Infosecurity magazine, August 07 2009. http://www.infosecurity-magazine.com/view/3094/pcidss-compliance-does-not-always-guarantee-security/.

36 W. Ashford. Nearly half of firms supporting BYOD report data breaches. ComputerWeekly.com, August 9 2012. http://www.computerweekly.com/news/2240161202/Nearly-half-of-firms-supporting-BYOD-report-data-breaches.

37 CSO. The Executive Guide to Data Loss Prevention. CSO Magazine, CSO Executive Guide, Summer 2010.

38 S. Liu, R. Kuhn. Data Loss Prevention. IT Pro, IEEE Computer Society, March/April 2010.

39 Ernst & Young. Data loss prevention. Insights on IT risk. Business briefing, October 2011.

40 Ernst & Young. Op. cit 40. Data loss prevention.

41 ComputerWeekly. Top Seven Data Loss Issues. ComputerWeekly.com, 2009. Disponible en http://www.computerweekly.com/feature/Top-seven-data-loss-issues.

42 J. Vijayan. TJX data breach: At 45.6M card numbers, it's the biggest ever. Computerworld, March 2007. http://www.computerworld.com/s/article/9014782/TJX_data_breach_At_45.6M_card_numbers_it_s_the_biggest_ever.

43 R. Kerber. Court filing in TJX breach doubles toll. The Boston Globe, October 24 3007. http://www.boston.com/business/globe/articles/2007/10/24/court_filing_in_tjx_breach_doubles_toll/.

44 J. Pereira. How Credit Card Data Went Out Wireless Door. The Wall Street Journal, May 4 2007. http://online.wsj.com/article/SB117824446226991797.html.

45 K. Jackson Higgings. Hacking the Real TJX Story. Information Week, online edition, March 15 2007. http://www.informationweek.com/security/government/hacking-the-real-tjx-story/208803414?queryText=TJX.

46 J. Vijayan. One year later: Five takeaways from the TJX breach. Computerworld, January 17 2008. http://www.computerworld.com/s/article/9057758/One_year_later_Five_takeaways_from_the_TJX_breach?taxonomyId=82&pageNumber=1.

ie foundation

La Fundación IE es un instrumento de IE para facilitar a los alumnos, profesores y staff el desarrollo de sus actividades formativas, investigadoras y de gestión.

Se orienta prioritariamente a la formación y la extensión cultural integral de cuantas personas o instituciones mantienen vínculos con IE.

Sus recursos están orientados a la financiación de becas para los estudiantes, ayudas para la formación e investigación de los profesores y fondos para la actualización y mejora de las estructuras educativas de IE.

Desarrolla sus tareas en todo el territorio español, pero mantiene una proyección y presencia internacionales en toda América, el sudeste Asiático, el Medio Oriente, el Norte de África y el continente Europeo.

iefoundation@ie.edu
www.ie.edu/foundation

ERNST & YOUNG

Ernst & Young es una firma líder mundial en servicios profesionales de auditoría, de asesoramiento fiscal y legal, transacciones y consultoría. Nuestros 167.000 profesionales comparten en todo el mundo una única escala de valores y un firme compromiso con la calidad. Contribuimos a afianzar el potencial de nuestra gente, nuestros clientes y otros grandes colectivos. Ernst & Young marca la diferencia.

Ernst & Young es una organización mundial constituida por firmas miembros de Ernst & Young Global Limited, cada una de las cuales es una entidad legal independiente. Ernst & Young Global Limited, compañía domiciliada en el Reino Unido, no presta servicios a clientes. Para más información, le invitamos a visitar www.ey.com

www.ey.com/es